AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS

1. (Currently Amended) A group management system comprising:

a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications between said interconnected nodes are encrypted; and

a plurality of master nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member nodes and further facilitating said communications between said plurality of interconnected nodes, wherein in the event one of the master nodes fails, the associated subset of member nodes will be automatically reassigned to one or more other of the master nodes.

2. (Previously Presented) The system of claim 1, wherein a membership change in at least one of the subsets can be performed without notifying all of the master nodes not associated with the changed subset.

3. (Previously Presented) The system of claim 1, wherein at least two of the subsets do not share any member nodes in common.

4. (Previously Presented) The system of claim 1, wherein at least two of the subsets share at least one member node in common.

5. (Previously Presented) The system of claim 4, wherein a communication involving said common member node can be transmitted along multiple paths.

6. (Original) The system of claim 5, further comprising an intrusion detection mechanism that receives said multiple-path communication as input.

7. (Cancelled)

8. (Currently Amended) The system of claim [[7]] 1, wherein each of the member nodes is associated with at least one of the master nodes as a back-up master.

9. (Previously Presented) The system of claim 1, wherein the plurality of interconnected nodes is communicatively coupled as part of a peer-to-peer network.

10. (Previously Presented) The system of claim 1, wherein the plurality of master nodes is part of an edge-based content delivery network.

11. (Previously Presented) The system of claim 1, wherein the member nodes are allocated to the subsets at least partly based upon one or more criteria of connectivity between each of the member nodes and the corresponding master nodes.

12. (Previously Presented) The system of claim 11, wherein the connectivity criteria are selected from a group of criteria comprising geographical distance, topological distance, bandwidth, latency, jitter, financial cost, and political boundaries.

13. (Previously Presented) The system of claim 1, wherein at least one of the master nodes further controls membership in another virtual overlay group different from the VPN.

14. (Previously Presented) The system of claim 1, wherein a communication from a first one of the subsets of the member nodes uses a first encryption key, and a communication from a second one of the subsets uses a second encryption key that is different from the first encryption key.

15. (Original) The system of claim 14, wherein one or more of the master nodes are

operable to translate between encryption keys.

16. (Previously Presented) The system of claim 1, wherein a communication from a first one of the subsets of the member nodes and a communication from a second one of the subsets of the member nodes both use the same encryption key.

17. (Previously Presented) The system of claim 1, wherein at least one of the master nodes is operable to remotely install software communication mechanisms for a new member node of the VPN without the necessity of installing augmented hardware for the new member node.

18. (Currently Amended) A method for managing a group, the method comprising:

providing a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications between said interconnected nodes are encrypted; and

providing a plurality of master nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member nodes and further facilitating said communications between said plurality of interconnected nodes, wherein in the event one of the master nodes fails, the associated subset of member nodes will be automatically reassigned to one or more other of the master nodes.

19. (Previously Presented) The method of claim 18, wherein a membership change in at least one of the subsets can be performed without notifying all of the master nodes not associated with the changed subset.

20. (Previously Presented) The method of claim 18, wherein at least two of the subsets do not share any member nodes in common.

21. (Previously Presented) The method of claim 18, wherein at least two of the

subsets share at least one member node in common.

22. (Previously Presented) The method of claim 21, wherein a communication involving said common member node can be transmitted along multiple paths.

23. (Previously Presented) The method of claim 22, further comprising an intrusion detection mechanism that receives said multiple-path communication as input.

24. (Cancelled)

25. (Currently Amended) The method of claim [[24]] 18, wherein each of the member nodes is associated with at least one of the master nodes as a back-up master.

26. (Previously Presented) The method of claim 18, wherein the plurality of interconnected nodes is communicatively coupled as part of a peer-to-peer network.

27. (Previously Presented) The method of claim 18, wherein the plurality of master nodes is part of an edge-based content delivery network.

28. (Previously Presented) The method of claim 18, wherein the member nodes are allocated to the subsets at least partly based upon one or more criteria of connectivity between each of the member nodes and the corresponding master nodes.

29. (Previously Presented) The method of claim 28, wherein the connectivity criteria are selected from a group of criteria comprising geographical distance, topological distance, bandwidth, latency, jitter, financial cost, and political boundaries.

30. (Previously Presented) The method of claim 18, wherein at least one of the master nodes further controls membership in another virtual overlay group different from the VPN.

31. (Previously Presented) The method of claim 18, wherein a communication from a first one of the subsets of the member nodes uses a first encryption key, and a communication from a second one of the subsets uses a second encryption key that is different from the first encryption key.

32. (Previously Presented) The method of claim 31, wherein one or more of the master nodes are operable to translate between encryption keys.

33. (Previously Presented) The method of claim 18, wherein a communication from a first one of the subsets of the member nodes and a communication from a second one of the subsets of the member nodes both use the same encryption key.

34. (Previously Presented) The method of claim 18, wherein at least one of the master nodes is operable to remotely install software communication mechanisms for a new member node of the VPN without the necessity of installing augmented hardware for the new member node.

35. (Currently Amended) A computer readable medium containing an executable program for managing a group, where the program performs the steps of:

providing a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications between said interconnected nodes are encrypted; and

providing a plurality of master nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member nodes and further facilitating said communications between said plurality of interconnected nodes, wherein in the event one of the master nodes fails, the associated subset of member nodes will be automatically reassigned to one or more other of the master nodes.

36. (Previously Presented) The computer readable medium of claim 35, wherein a membership change in at least one of the subsets can be performed without notifying all of the master nodes not associated with the changed subset.

37. (Previously Presented) The computer readable medium of claim 35, wherein at least two of the subsets do not share any member nodes in common.

38. (Previously Presented) The computer readable medium of claim 35, wherein at least two of the subsets share at least one member node in common.

39. (Previously Presented) The computer readable medium of claim 38, wherein a communication involving said common member node can be transmitted along multiple paths.

40. (Previously Presented) The computer readable medium of claim 39, further comprising an intrusion detection mechanism that receives said multiple-path communication as input.

41. (Cancelled)

42. (Currently Amended) The computer readable medium of claim [[41]] 35, wherein each of the member nodes is associated with at least one of the master nodes as a back-up master.

43. (Previously Presented) The computer readable medium of claim 35, wherein the plurality of interconnected nodes is communicatively coupled as part of a peer-to-peer network.

44. (Previously Presented) The computer readable medium of claim 35, wherein the plurality of master nodes is part of an edge-based content delivery network.

45. (Previously Presented) The computer readable medium of claim 35, wherein the member nodes are allocated to the subsets at least partly based upon one or more criteria of connectivity between each of the member nodes and the corresponding master nodes.

46. (Previously Presented) The computer readable medium of claim 45, wherein the connectivity criteria are selected from a group of criteria comprising geographical distance, topological distance, bandwidth, latency, jitter, financial cost, and political boundaries.

47. (Previously Presented) The computer readable medium of claim 35, wherein at least one of the master nodes further controls membership in another virtual overlay group different from the VPN.

48. (Previously Presented) The computer readable medium of claim 35, wherein a communication from a first one of the subsets of the member nodes uses a first encryption key, and a communication from a second one of the subsets uses a second encryption key that is different from the first encryption key.

49. (Previously Presented) The computer readable medium of claim 48, wherein one or more of the master nodes are operable to translate between encryption keys.

50. (Previously Presented) The computer readable medium of claim 35, wherein a communication from a first one of the subsets of the member nodes and a communication from a second one of the subsets of the member nodes both use the same encryption key.

51. (Previously Presented) The computer readable medium of claim 35, wherein at least one of the master nodes is operable to remotely install software communication

mechanisms for a new member node of the VPN without the necessity of installing augmented hardware for the new member node.